UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

IN THE MATTER OF THE SEARCH OF:	)	
RESIDENTIAL PROPERTY LOCATED AT	)	**Case No. 3:23-MJ-** 1127
109 S. GALLAHER VIEW RD., APT. NO. 143	)	
KNOXVILLE, TENNESSEE 37919	)	
AND THE BLUE TOYOTA SIENNA	)	
MINIVAN, TENNESSEE TAG 343BGQD	)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your affiant, Thomas Evans, an Investigator with the Knoxville Police Department (KPD) Internet Crimes against Children (ICAC) Task Force and being a Task Force Officer with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) being duly sworn, deposes and states the following:

1. Your affiant has been employed with the KPD since January 22, 1996. Your affiant has been assigned to the Knoxville Police Department's Internet Crimes Against Children Task Force (KPD-ICAC) as a computer examiner and undercover online investigator for the past twenty-three years. The KPD-ICAC Task Force is responsible for investigating and enforcing federal criminal statutes involving the sexual exploitation of children under Title 18, United States Code, Chapter 110, including, without limitation, sections 2251(a), 2252A(a)(5)(B), and 2422(b).

2. Your affiant has acquired experience in these matters through specialized training and everyday work related to these types of investigations. Your affiant has completed the following training:

1996 Knoxville Police Department Training Academy Recruit Class A.

1997 Childhelp USA's Professional Training Conference.
1999 Protecting Children On-line provided by Fox Valley Technical College Criminal Justice Department, Appleton Wisconsin.

2000 Advanced Protecting Children On-line provided by Fox Valley Technical College, Criminal Justice Department.

2000 National Consortium of Justice Information and Statistics Training directed toward on-line investigation, tracking offenders and data recovery.

2000 40-hour course in the National White Collar Crime Data Recovery and Analysis.

2000 40-hour Internship with the Dallas Police Department's Internet Crimes Against Children Task Force.

40-hour internship with the Maryland State Police in October 2000 focusing on forensic software use in recovering computer-based evidence.

2001 Basic Class on EnCase computer forensic software.

2001 National Internet Crimes Against Children Training Conference in New Orleans focusing on the use of computer forensic utilities in evidence collection and Online Investigative Techniques.

2002 Crimes Against Children Conference in Dallas, TX focusing on online investigative techniques and computer forensic data recovery.

40-hour EnCase Intermediate Analysis and Reporting training in Sterling, VA April 2003.

2004 Silicon Valley ICAC Task Force Conference in San Jose, Ca with focus on online investigations and best computer forensic practices.

2004 Crimes Against Children Conference in Dallas, TX with emphasis on online investigative techniques and data recovery.

December 2004 ICAC Investigative Techniques course in Knoxville, TN focusing on updated investigative techniques in online undercover operations.

March 2005 EnCase Intermediate Analysis and Reporting course for computer examiners in Sterling, VA.

May 2005 International Association of Computer Investigative Specialist 80-hour Forensic Computer Examiner Training Program in Orlando, FL.

Recognized in April 2005 by the International Association of Computer Investigative Specialists as a Certified Electronic Evidence Collection Specialist.

2005 National ICAC Conference in Dallas, TX focusing on characteristics of the Internet offender and online undercover operations.

Knoxville Police Department Basic Investigator Class January 30- February 3, 2006.

2006 National Crimes Against Children Conference in Dallas, TX focusing on online undercover Investigative Techniques.

December 2006 FTK Boot camp held at Pellissippi State Technical College for computer forensic training using the Access Data Ultimate Toolkit software package.

January 2007 Internet Crimes Against Children Task Force Operation Peer Precision Training in Tallahassee FL focusing on online undercover Peer-to-Peer investigations.

June 12, 2008 F.B.I. CART ImageScan training concentrating on the use of the ImageScan System for secure computer previews and data recovery.

April 11- May 14th 2010 United States Secret Service BCERT Computer Forensic training Hoover, AL.

January 2011 assigned to the United States Secret Service Electronic Crimes Task Force for East Tennessee.

February 21-23rd 2012 Tennessee ICAC Training conference in Nashville, TN focusing on cell phone investigations, human trafficking, undercover P2P investigations (instructed), and open-source computer forensic tools.

USDOJ 2012 National Law Enforcement Training Conference in Atlanta GA April 17-19th, 2012 focusing on P2P undercover investigations, Craigslist undercover investigations, Gigatribe investigations, and the psychological profile of a child pornography collector.

June 13-17th Internship with the Citrus County Sheriff's Department regarding E Commerce undercover investigations (Operation Summer Nights).

February 5th - 8th 2013 ICAC eMule P2P investigations.

March 26-28th 2013 – Tennessee ICAC state conference in Nashville, TN focusing on Commercial Sexual Exploitation of Children (CSEC).

October 28-31, 2013 Tennessee ICAC state conference in Nashville, Tennessee, focusing on forensic preview tools, ICAC legal updates and virtual machine utilization for computer forensics and undercover investigations.

February 24-26, 2014 – Tennessee ICAC state conference in Nashville, TN, focusing on computer previews, Google Security, and locating wireless devices.

April 15-17, 2014 – 2014 Regional ICAC Law Enforcement Training on Child Exploitation focusing in court testimony, Ares Peer to Peer investigations, National Center for Missing and Exploited Children Law Enforcement Portal, and characteristics of the offender.

September 18-19, 2014 – Westminster, Colorado ICAC BitTorrent Investigations.

April 20-22, 2015 – Brentwood, Tennessee – Tennessee ICAC state conference focusing on online undercover chat investigations, legal updates, and human sex trafficking.

November 11-13, 2015 – Gatlinburg, Tennessee – Tennessee ICAC conference focusing on current chat trends, P2P file sharing investigations, and on scene preview techniques and software.

March 28-30, 2016 – Nashville, Tennessee – Tennessee ICAC conference focusing on legal updates, use of polygraph in conjunction with child pornography cases and online undercover operations.

April 18, 2016 – Atlanta, Georgia – National ICAC Conference focusing on online undercover investigations, interviewing offenders, legal updates, psychology of the internet offender and on scene computer forensic tools.

May 2, 2016 – Knoxville, Tennessee – Federal Bureau of Investigation Legal Training.

October 17-19, 2016 – Chattanooga, Tennessee – Tennessee ICAC State Conference focusing on Legal Updates, Anonymity and Darknet, and IP Version 6.

February 27- February 28, 2017 – Atlanta, Georgia – Darknet Training. Training focused on anonymous Darknet applications for the trafficking of child pornography.

3. As a federal task force officer, your affiant is authorized to investigate violations of the laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. This affidavit is made in support of an application for a warrant to search the premises located at 109 S. Gallaher View Rd., Apt. No. 143, Knoxville, TN 37919. This residence

is more particularly described in ATTACHMENT A, a copy of which is attached hereto and incorporated by reference herein.

5. Information contained within the affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning the investigation. I have set forth only the facts which I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2251(a), 2252A(a)(5)(B), and 2422(b) described in ATTACHMENT B, are presently located at the premises described in ATTACHMENT A.

GLOSSARY OF TERMS APPLICABLE TO THIS AFFIDAVIT

6. INTERNET SERVICE PROVIDER (ISP): A company that provides its customers with access to the Internet, usually over telephone lines or cable connections. Typically, the customer pays a monthly fee, and the ISP supplies software and/or hardware that enables the customer to connect to the Internet by a modem or similar device attached to or installed in a computer.

7. THE INTERNET: The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across county, state, and national boundaries.

8. INTERNET PROTOCOL ADDRESS (IP Address): The unique numeric address of a machine or computer attached to and using the Internet. This address is displayed in four

blocks of numbers, e.g., 123.456.789.001. One computer or device can only use each numbered IP address over the Internet at a time.

9. KiK: KiK is a free-access anonymous social media application and online platform where users engage in conversations without identities or profiles. KiK users can create groups where like-minded users can gather to communicate and share media files. Additionally, KiK can be used on computers and/or smartphones.

10. P2P: P2P, or peer-to-peer, is a network in which computers communicate directly with one another rather than routing traffic through managed central servers and networks.

11. ACCURINT: Accurint is a widely used and accepted as a tool to locate and research publicly available records. Accurint is used by government, commercial, and law enforcement agencies to obtain publicly available information and has been utilized by myself numerous times in previous investigations. Accurint has proved reliable in each previous investigation.

12. SNAPCHAT: Snapchat is a widely used and popular instant messaging application. Snapchat is typically downloaded and used on smartphones but a web version can be used from a computer. A primary feature of Snapchat is that pictures and messages are only available for short periods of time before becoming inaccessible.

13. AVATAR: an icon or figure representing a particular person in video games, internet forums, or other social media.

COMPUTERS/SMARTPHONES AND CHILD PORNOGRAPHY

14. Your affiant has received extensive online undercover training as well as computer forensics training in reference to computer-related criminal investigations. Your affiant knows all of the below-described information as the result of his training and experience in the investigation

of computer-related crime and by conferring with other law enforcement personnel who investigate computer-related crime.

15. Your affiant knows that, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It also has revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

16. The advancement in technology of computers, smartphones and tablets has added to the methods used by child pornography collectors to interact with and sexually exploit children. Each of the above serves six functions in connection with child pornography. These are: production, communication, distribution, receipt, advertisement, and storage.

17. Child pornographers can now produce both still and moving images directly from a common video camera, small action style cameras such as a GoPro, smartphones, laptop computers equipped with web cameras, and tablets. In the past, a camera could be attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred, or printed directly from the computer, external hard drive,

media card (SD, Compact Flash, micro-SD, memory stick), smart phone, tablet, iPod, or iPad. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is inexpensive and technically easy to produce, store, and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow, as had been the case in the past. Your affiant has been involved in recent investigations where digital cameras, smart phones, tablets, and webcams were used to produce child pornography and store said child pornography either on the device, personal computer or removable media of the subject.

18. New technology now allows child pornographers to use even smaller digital devices like smartphones and tablets that have digital cameras and video recording capability built directly into the devices. These devices are equipped with their own processors and memory that allow the devices to actually perform as small mini computers. With the use of free and publicly available applications, a child pornographer has the ability to produce child pornography, receive and distribute it in a matter of just a few seconds and maintain relative anonymity using free open wireless access points.

19. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer also has changed that. A device known as a modem allows any computer to connect to another computer through the use of telephone and/or cable lines. By connecting to a host computer, electronic contact can be made with literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host

computers are sometimes operated by commercial concerns, such as Bellsouth, AT&T and America Online, which allow subscribers to dial a local number and connect to a network which is in turn connected to their host systems. Today many ISPs, such as Comcast Communications and Charter Communications, offer high-speed broadband Internet service. Broadband is often called high-speed Internet because it usually has a high rate of data transmission much higher than the dial-up or DSL structure of the past. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web. Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms" and/or instant messaging.

20. These communication structures are ideal for individuals who possess, receive and distribute child pornography. They provide open and anonymous communication, allowing users to locate other persons who share their interest in child pornography, while maintaining their anonymity. Once contact has been established, it is then possible to send text messages, graphic images, and high-resolution video to other individuals interested in child pornography. Moreover, the child pornographer need not use the large service providers. Child pornographers can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. Or commonly used today, such as applications that can be downloaded and installed on smartphones. Applications such as Discord,[1] KiK, and Omegle[2] are examples of applications that are commonly used on smartphones. These communication links allow contacts around the world as easily as calling next

[1] Discord is an instant messaging and Voice Over IP (VoIP) social platform. Users have the ability to communicate with voice calls, video calls, text messaging, media, and files in private chats or as part of communities called "servers." *See* https://www.discord.com.

[2] Omegle is a free online chat website that allows users to socialize with others without the need to register. The service randomly pairs users in one-on-one chat sessions where they chat anonymously using the names "You" and "Stranger." *See* https://www.omegle.com.

door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well-known and are the foundation of transactions and communications between child pornographers.

21. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred via electronic mail to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, P2P services, and easy access to the Internet, computers, tablets, and smartphones are a preferred method of receipt and distribution of child pornographic materials.

22. A computer and/or a smartphone's capability to store images in digital form makes them an ideal repository for child pornography. The size of the electronic storage media (commonly consisting of hard drives) used in home computers has grown tremendously within the last several years as have the storage capacities of smartphones. Hard drives with the capacity of two terabytes are not uncommon. The KPD-ICAC computer examiners routinely examine computer hard drives of 1 Terabyte (1000 gigabytes) and more in child pornography cases. It is not uncommon today for examiners to also examine multiple smartphones during an investigation as they are ideal for trafficking in child pornography and being mobile. These drives/devices can store hundreds of thousands of images and video at very high resolution and quality. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, save the image, and store it at another location. Once this is done, there is no readily apparent

evidence at the scene of the crime. Only with careful examination of electronic storage devices is it possible to recreate the evidence trail.

23. Based on your affiant's knowledge, training and experience and training and experience of other officers, your affiant knows that child pornographers commonly download and save some of their collection of child pornography from their computer to removable media such as thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, smart televisions, computer game consoles (Sony PlayStation, Xbox), tablets, iPods or iPads so the images can be maintained in a manner that is both mobile and easily accessible to the collector. It is not uncommon for the child pornographer to print pictures of child pornography and to keep them in a safe and secure location for easy viewing. Thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro-SD, memory stick), smart phones, smart televisions, computer game consoles (Sony PlayStation, Xbox), tablets, iPod's, or iPads, containing child pornography and printed pictures of child pornography are not only kept near the computer, but also in hidden areas known to the child pornographer, to keep other individuals from discovering the illegal material. For example, a search warrant executed by other officers known to your affiant resulted in the finding of a hard drive wrapped in plastic hidden under a bathroom sink. Additionally, your affiant knows that in 2014, investigators with the KPD-ICAC Task Force arrested a subject for the interstate travel to meet a minor for sexual purposes (18 U.S.C. § 2423(a)). An external hard drive was located in the trunk of the suspect vehicle. A search warrant on the external hard drive revealed a contact offense by the subject on a four-year-old girl and numerous pornographic videos of the sexual abuse produced by the subject utilizing his smartphone.

24. Your affiant states that computer technology can be mobile in the form of laptop computers, removable thumb drives, removable hard drives, media cards (SD, Compact Flash, micro-SD, memory stick), computer game consoles (Sony PlayStation, Microsoft Xbox), smart phones, iPad's, iPod's, tablets, or accessible via remote or wireless means. Therefore, evidence, contraband, instrumentalities, or fruits of crime can be located virtually anywhere within the residence or vehicle of a child pornographer. Your affiant has been involved in child pornography investigations where child pornography was found on removable media located in a suspect's vehicle. Your affiant has also been involved in investigations where smartphone (Android) emulators were utilized on a computer to allow the user to use applications that had been installed and utilized on the subject's smartphone. Additionally, child pornography can remain on devices indefinitely unless the user takes active steps to delete or overwrite the digital files of child pornography. Your affiant is aware of a Knoxville Police Department ICAC investigation that originated as a P2P file-sharing investigation in 2015. The computer examination in this case has located child pornography files stored on the suspect computer hard drive dating back to 2009. Additionally, recent investigations have revealed that some P2P suspects in order to remain safer have instituted the methodology of downloading child pornography then deleting it after a short period of time. Your affiant knows based on information gained from interviews with child pornographers that utilized the above-described method, the suspects indicated they felt an increased level of security knowing the child pornography was not stored on the computer/devices for long periods of time and that they could re-download mass amounts of child pornography at any time. However, computer examinations have revealed that, even if the above methodology is utilized, examiners are able to locate and recover evidence about the criminal activity including, but not limited to, the files child pornography, software used to locate and download child

pornography, log files identifying specific child pornography files that have been downloaded and chat/messaging conversations that have occurred through use of the suspect computer system.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

25. Based on your affiant's training and experience, your affiant knows that the search of computers and retrieval of data from computer systems and related media, often requires agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a) Computer storage devices like thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro-SD, memory stick), smart phones, smart televisions, computer gaming consoles (Sony PlayStation, Xbox), tablets, iPods or iPads can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b) Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed,

password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from a destructive code imbedded in the system such as a "booby trap," a controlled environment is essential to its complete and accurate analysis.

26. Based upon your affiant's training and experience and consultation with experts in computer searches, data retrieval from computers, and related media, as well as consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all computer system input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the systems data in a laboratory or other controlled environment. This is true because of the following:

a) The peripheral devices, which allow users to enter or retrieve data from the storage devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, and/or data security devices are not necessary to retrieve and preserve the data after inspection, the government will return the material in a reasonable time.

b) In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit. Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c) The Knoxville Police Department's ICAC Task Force, currently conducts onsite previews of computers and smart phones in order to focus and seize only devices containing contraband. This process assists investigators with only seizing and examining items associated with the criminal activity. Based on experience, cooperation from occupants of the residence being searched assists investigators with identifying and seizing only devices that will contain contraband. It is important to note that systems currently powered off will not be powered on to conduct a preview unless investigators believe turning on the device will not alter or destroy possible evidence.

27. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime of advertising, distribution, receipt, and/or possession of child pornography in violation of the law and should all be seized as such.

28. Based on your affiant's training and experience in computer searches and data retrieval from computers while in a laboratory setting, your affiant is aware that such searches can be complex and time consuming.

PROBABLE CAUSE

29. This affidavit is submitted in support of the issuance of a warrant authorizing the search of the premises described in ATTACHMENT A, along with the digital media found there, in order to locate and seize the items described in ATTACHMENT B.

30. On or about August 3, 2022, your affiant received information from federal law enforcement regarding an undercover operation investigating the sexual exploitation of minors. Through this information I learned that undercover officers had engaged in online conversations with the Kik user "SuperCoolDaddy" whereby SuperCoolDaddy and the undercover officer discussed the sale of a minor female for sex. During one of these conversations, SuperCoolDaddy sent the undercover officer a video file that depicted child pornography.

31. Your affiant reviewed that video file that depicted child pornography and is described as follows:

> File Name: IMG_1669.MP4 – An adult-male inserts his erect penis into the mouth of a minor female approximately five years old. The female minor's face is not clearly visible. The camera zooms out as the video progresses to show the minor's vagina. The video is a color video with sound and is approximately thirty seconds in length.

32. On or about August 08, 2022, your affiant received information from Metro Nashville Police Department regarding the National Center For Missing and Exploited Children (NCMEC) Cybertip #128572234. The NCMEC Cybertip stated that the KiK user "SuperCoolDaddy," with email address of harrisjake176@gmail.com, had distributed two video files, one of which depicted child pornography.

33. Your affiant reviewed the video file that depicted child pornography and confirmed that it was the same video file SuperCoolDaddy sent to federal undercover law enforcement officers during the above-described undercover operation described in paragraph 30, above.

34. As part of his initial investigation, Metro Nashville Detective Robert Carrigan issued a subpoena for subscriber records to KiK for the user "SuperCoolDaddy." KiK responded with the following information:

First Name: SuperCoolDad

Last Name:

Email: harrisjake176@gmail.com (confirmed)

Registration Client: Android OnePlus

35. Additionally, KiK provided IP logs of user login times and the particular IP address at the time of upload of the child pornography file. The IP addresses that "SuperCoolDaddy" used to access KiK and upload the child pornography file resolved to T-Mobile.

36. Detective Carrigan obtained a State of Tennessee Judicial Subpoena for subscriber information from T-Mobile on the following IP addresses used by "SuperCoolDaddy" to access the KiK:

2607:fb91:2f9b:e3b2:a8f7:96ed:b274:8a6b on 07/11/22 at 20:56:57 UTC

2607:fb91:2f19:feb2:80ea:8b4f:85a266b9 on 07/02/22 at 19:37:11 UTC

2607:fb91:2f1d:9790:4858:345:c449:716c on 06/28/22 at 18:02:30 UTC

37. T-Mobile responded to the subpoena request with the following subscriber information:

Subscriber Name: Jennifer Parker

Subscriber Address: 1001 Dunhill Way Apt. 204 Knoxville, TN

Subscriber Status: Active

Subscriber Name Effective Date: 05/06/2021

38. Metro Nashville Police Detective Carrigan, on receiving information from T-Mobile regarding the subscriber Jennifer Parker at 1001 Dunhill Way Apt. 204 Knoxville, TN, forwarded information to your affiant for follow-up investigation.

39. Upon receiving the case information from Detective Carrigan, your affiant made contact with the apartment manager at Dunhill Apartments regarding Jennifer Parker and other possible occupants in apartment 204. The management advised that Parker had resided there but was evicted when the management learned that Darrell Moore (DOB:03/05/1982), who was residing with Parker, had a felony arrest and he was not on the lease.

40. Through investigation your affiant determined that Darrell Moore and Jennifer Parker are currently residing at the InTown Suites Apartment 143, 109 S. Gallaher View Rd., Knoxville, TN 37919, and have been residing in Apartment 143 since October, 2022.

41. On 07/03/2023 your affiant spoke to the manager at the InTown Suites regarding Parker and Moore. The manager confirmed they had been living in Apartment 143 since October of 2022 and that they had been good tenants. The manager also stated that recently the lease had been changed from Jennifer Parker's name to Darrell Moore's name. The manager stated that they were in the apartment most of the time. He stated that he did not know Moore to have a vehicle.

42. Your affiant showed photographs of Jennifer Parker (DOB 08/28/1990) and Darrell Moore (03/05/1982) to the manager and he confirmed that those were the individuals living in Apartment 143.

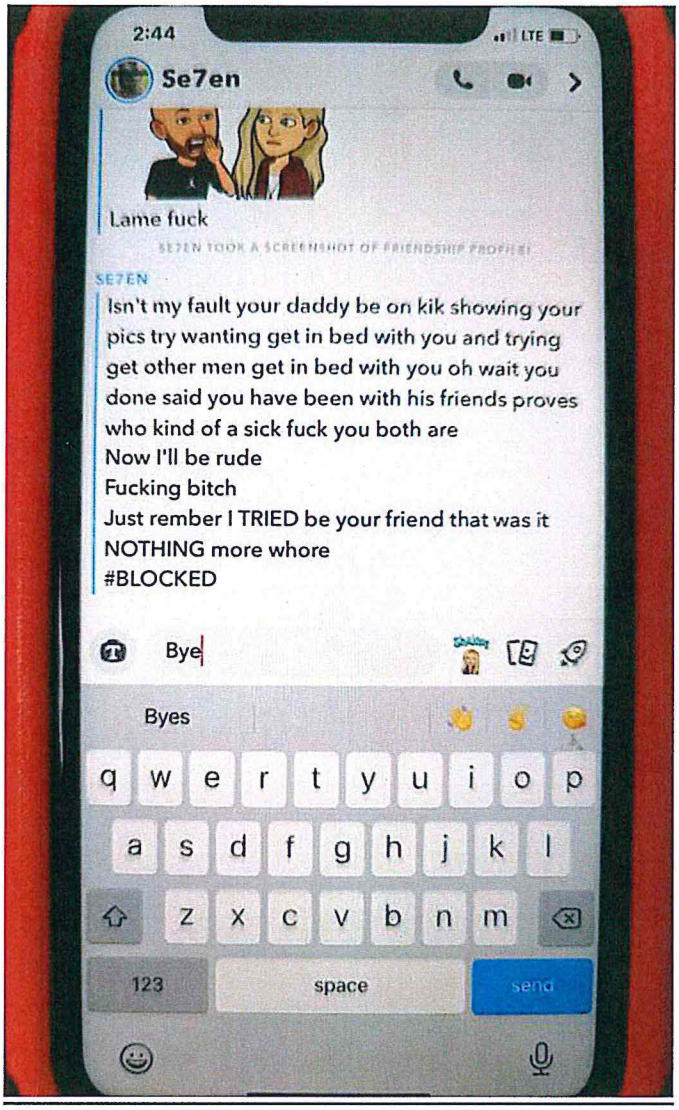
43. Your affiant conducted surveillance at the InTown Suites at various times between 06/01/2023 and 07/13/2023 and noted that a blue Toyota Sienna minivan TN license 343BGQD

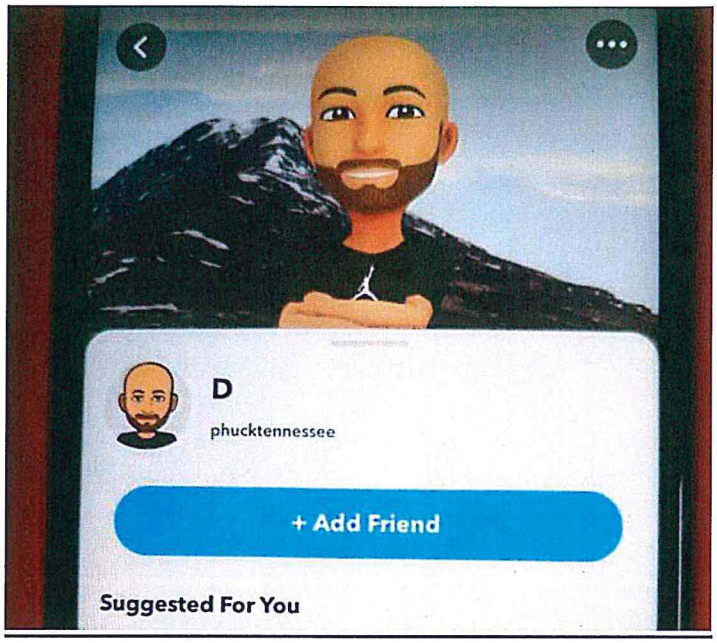
was usually parked in front of Apartment 143. A check of the Tennessee Criminal Justice Portal showed that the TN license plate number of 343BGQD is registered to Jennifer Parker at 1001 Dunhill Way Apt 204, Knoxville, TN 37917. This was the previous address of both Jennifer Parker and Darrell Moore.

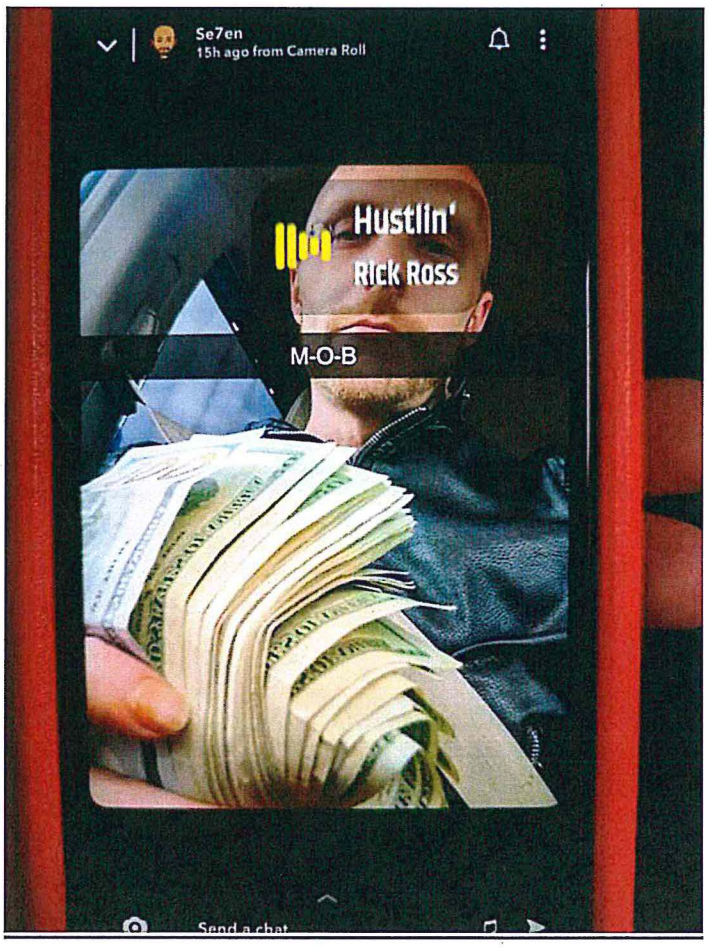
44. On or about 06/09/2023 your affiant, while conducting surveillance at the InTown Suites, saw Jennifer Parker leave apartment 143 with a minor child and get into the blue Toyota Sienna minivan TN license 343BGQD that was registered to her.

45. As referenced in paragraph 30, above, your affiant learned that during this same time frame that the FBI was investigating the Kik user "SuperCoolDaddy" as a subject of interest in an online enticement case. During the FBI investigation, the user "SuperCoolDaddy" also used the Snapchat account of "Se7en."

46. Most recently, on or about May 8, 2023, your affiant learned that the FBI had further communication with "SuperCoolDaddy" aka Snapchat user "Se7en." The FBI provided the following screen captures of the Snapchat user "Se7en" aka "SuperCoolDaddy":


2:44
LTE
Se7en
Lame fuck
SE7EN TOOK A SCREENSHOT OF FRIENDSHIP PROFILE!
SE7EN
Isn't my fault your daddy be on kik showing your pics try wanting get in bed with you and trying get other men get in bed with you oh wait you done said you have been with his friends proves who kind of a sick fuck you both are
Now I'll be rude
Fucking bitch
Just rember I TRIED be your friend that was it
NOTHING more whore
#BLOCKED
Bye
Byes
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
send


D
phucktennessee
+ Add Friend
Suggested For You


Se7en
15h ago from Camera Roll
Hustlin'
Rick Ross
M-O-B
Send a chat

47. In addition to the Snapchat user "Se7en" listing his name as "D," as in Darrell, he also lists "phucktennessee," which I believe reveals his location, and corroborates the IP addresses used to disseminate child sexual abuse material described above. Further, FBI Special Agent Ryan Malone, who is familiar with the above investigation, confirmed that the KiK user "SuperCoolDaddy" and Snapchat user "Se7en" were the same person-based FBI communication with the target.

48. Your affiant compared the photograph sent via Snapchat by "Se7en" aka as KiK user "SuperCoolDaddy" with the Tennessee Driver license photo of Darrell Moore (DOB 03/05/1982) and confirmed the two images of are the same person.

49. Additionally, today, August 1, 2023, I visited the SnapChat website and confirmed that the "D"/"phucktennessee" account displayed the same avatar as described in paragraph 46, above, and closely mirrors how Darrell Moore appears in his driver's license photo. Based on my training and experience, this demonstrates that the account in still active.

50. Based on the aforementioned factual information, and my training and experience, your affiant respectfully submits that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a), and 2252A(a) are located on computers or electronic devices located at 109 South Gallaher View Rd. Apt 143, Knoxville, TN 37919.

51. Your affiant bases this belief on the fact that on 07/08/2022, KiK identified (1) video file of child pornography that was transmitted via KiK Messenger. The video file was distributed by the KiK user "SuperCoolDaddy" with email account of harrisjake176@gmail.com. KiK made Cybertip 128572234 to the National Center for Missing and Exploited Children. Additionally, KiK provided past login IP addresses and times for the user known as

"SuperCoolDaddy" with email account of harrisjake176@gmail.com. A subpoena for records was issued to T-Mobile for subscriber information pertaining to the IP addresses of:

2607:fb91:2f9b:e3b2:a8f7:96ed:b274:8a6b on 07/11/22 at 20:56:57 UTC, 2607:fb91:2f19:feb2:80ea:8b4f:85a266b9 on 07/02/22 at 19:37:11 UTC, and 2607:fb91:2f1d:9790:4858:345:c449:716c on 06/28/22 at 18:02:30 UTC.

52. The subscriber of the T-Mobile services was identified as Jennifer Parker who during the time period of the above-described FBI enticement investigation, resided with Darrell More at 1001 Dunhill Way, Apt. 204 Knoxville, TN and who continues to reside with reside with Darrell Moore at the subject location: 109 South Gallaher View Rd, Apt 143, Knoxville, TN 37919.

53. Within the past three months, the SnapChat account "D"/ "phucktennessee" has had conversations with the FBI and is still an active account. A Tennessee Driver license photo of Darrell Moore (DOB 03/05/1982) confirmed the two images of are the same person and closely resemble the avatar for the above-described SnapChat account.

54. Based on the investigation, the above listed KiK account and Gmail account are associated with the upload of the CSAM video files by a particular T-Mobile user currently residing at the InTown Suites 109 South Gallaher View Rd. Apt.143, Knoxville, TN 37919. Your affiant knows from experience that anyone can create a Gmail email account and use Google services. Additionally, your affiant knows that KiK is often used to trade and collect child pornography and that anyone can create and use a KiK Messenger account. Your affiant knows from experience that most often individuals participating in the sexual exploitation of children by the collecting and trading of child pornography almost exclusively create fictitious accounts to indulge in criminal activity. Although the IP address is an excellent source of information where

the physical criminal activity has occurred, it cannot pinpoint which person within the household is the criminal suspect. Your affiant knows from personal experience that the offender literally could be anyone in the household to include one or both parents, sons and daughters (both minors and adult children) and other unknown persons living in the home. Your affiant knows from experience that devices in the home are sometimes shared between users, that old devices such as smart phones and laptops although no longer used can still access WiFi internet signals and be used by the offender to traffic in child pornography. Your affiant knows from experience that to successfully identify the offending device or devices that all of the devices in the residence may need to be examined or previewed onsite. Your affiant does not want to seize every piece of electronic equipment in the household or in the vehicles listed, however, it is critical that the process described in paragraph 25 be utilized to locate the offending device or devices. It has been your affiant's experience, that the on-scene screening process is less intrusive and less burdensome to the innocent individuals in the household who can quickly have their electronic devices returned to them.

55. Based on the experience and knowledge of these cases, your affiant believes there is probable cause to believe that the electronic devices which are most likely portable (such as laptop computers and cell phones) could possibly be stored in the following vehicle: blue Toyota Sienna minivan TN license 343BGQD registered to Jennifer Parker currently residing with Darrell Moore at the InTown Suites Apartment 143 at 109 South Gallaher View Rd, Knoxville, TN 37919. Your affiant has investigated a case where the subject had stored images of the sexual abuse of his girlfriend's minor daughter on an external hard drive and transported that hard drive in the trunk of his car to Knoxville, Tennessee.

56. Based on the foregoing, there is probable cause to believe that a computer and/or electronic device located at 109 South Gallaher View Rd. Apt. 143, Knoxville, TN 37919 has been used in conjunction with violations of, Title 18, United States Code, Section, 2252A(a)(1), which makes it a crime for any person to ship or transport child pornography in interstate or foreign commerce; Title 18, United States Code, Section 2252A(a)(2), which makes it a crime to knowingly receive or distribute child pornography that has traveled in interstate and foreign commerce; and Title 18, United States Code, Section 2252A(a)(5), which makes it a crime for any person to knowingly possess or access with intent to view material that contains an image of child pornography, as defined in Title 18, United States Code, Section 2256(8).

57. Further, there is probable cause to believe that evidence, fruits, and instrumentalities of this crime, which are listed specifically in Attachment B, which is incorporated herein by reference, are presently located on the premises described in Attachment A. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time and to examine, analyze and test them.

58. The evidence, fruits, and instrumentalities of violation of Title 18, United States Code, Section 2251, believed to be concealed at the premises described in Attachment A, are listed in Attachment B of this affidavit, which is incorporated herein.

59. Therefore, your affiant respectfully requests issuance of a search warrant authorizing the search and seizure of the items listed in Attachment B.

Tom Evans
Detective
Knoxville Police Department
Internet Crimes Against Children Task Force
Homeland Security Investigations Task Force

Subscribed and sworn to before me this 2nd day of August 2023.

Honorable Debra C. Poplin
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

Premises:

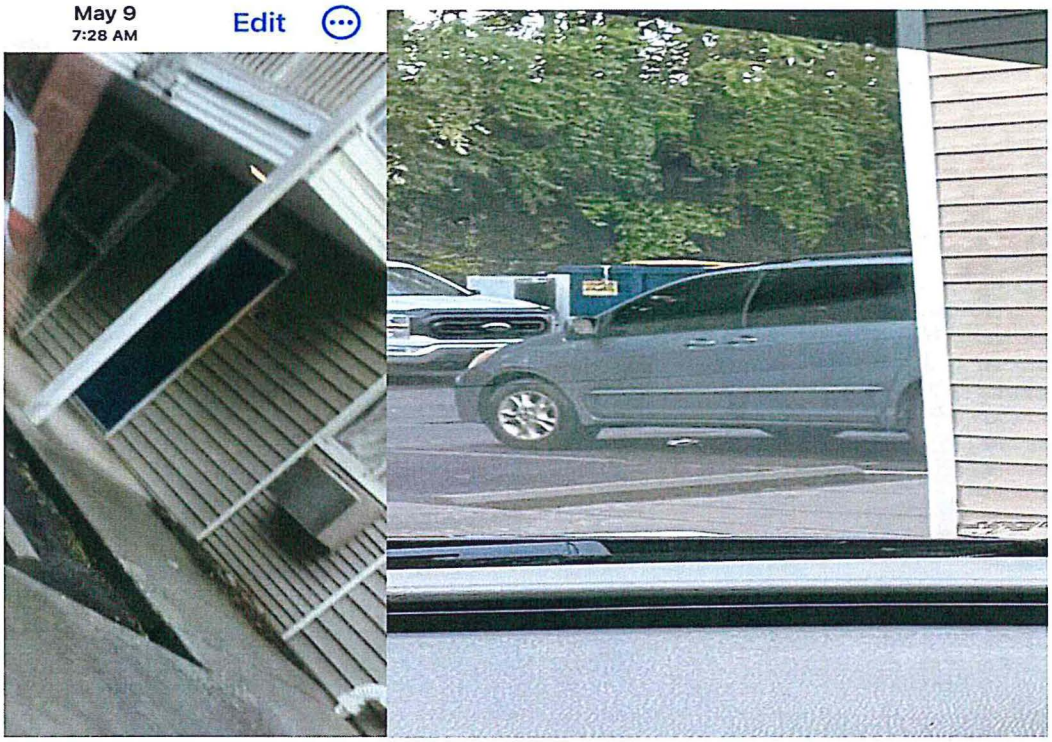
Apartment # 143 at the InTown Suites Extended Stay located at 109 S Gallaher View Rd., Knoxville, TN 37919 in the Eastern District of Tennessee, for any computer/device(s), computer-related media and smartphones located on the premises and within the blue Toyota Sienna TN tag 343BGQD.

Physical Description of Premises:

See Attached photo of apartment # 143 of the InTown Suites Extended Stay building located at 109 S Gallaher View Rd., Knoxville, TN 37919. See attached photograph of Toyota Sienna TN Tag 343BGQD.

Premises Location:

The InTown Suites Extended Stay is located at 109 S Gallaher View Rd., Knoxville, TN 37919. Apartment #143 is located on the ground floor on the South East side of the building. The apartment has a blue door and the number 143 to the right of the door. Windows on either side of the door with what appears to be an air conditioning/heating unit under the window to the right of the door. The Toyota Sienna TN Tag 343BGQD is usually parked in the parking lot of the apartment complex in front of or near apartment #143.



ATTACHMENT B

Below is a list of items to be searched and seized from the premises described in ATTACHMENT A:

1. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, video recording devices, video recording players, monitors and or televisions, flatbed scanners and data where instrumentalities of and will contain evidence related to this crime. The following definitions apply to the terms as set out in this attachment:

(a) Computer Hardware:

Computer hardware consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to central processing units; internal and peripheral storage devices such as thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, smart televisions, computer game consoles (Sony PlayStation, Xbox), tablets, iPods or iPads, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printers, video display monitors, and related communication devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

(b) Computer Software:

Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

(c) Documentation:

Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

(d) Passwords and Data Security Devices:

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress,

hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

1. Child pornography in any form.

2. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18, United States Code, Section 2256(8).

3. Any and all correspondence identifying persons transmitting, through interstate commerce including the United States mail or computers, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

4. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).